NRD Cyber Security

Key pillars for effective CSIRT establishment

www.nrdcs.eu

Professional background

About me: Dr Tadas Jakstas

Team lead, cybersecurity capacity building at NRD Cyber Security

10 years of experience in managing cybersecurity capacity/CSIRT establishment projects all around the world

Experience working for international organisations (World Bank, NATO, the EU,) and public sector (LTU MoD, Crisis Management Bureau)

Certified SOC CMM Assessor

Trainer at SECO Institute and ITU training academy - Crisis Management Foundation course

Regular speaker and author of various cybersecurity capacity building best practice publications

My capacity building/CSIRT projects

- Serbia
- Qatar
- Ukraine
- Greece (ENISA)
- Serbia
- Bosnia and Herzegovina
- North Macedonia
- Saudi Arabia
- Switzerland
- Bangladesh
- Sri Lanka
- Equador
- The Bahamas
- Bhutan
- Tajikistan
- Albania
- Kyrgyzstan
- Mongolia
- Rwanda
- Togo
- Benin
- Cote D'Ivoire
- Mauritania
- São Tomé and Príncipe
- Gambia
- Senegal
- Cape Verde
- Malawi
- Lithuania
- Armenia
- Bhutan

NRD Cyber Security

FOCUS

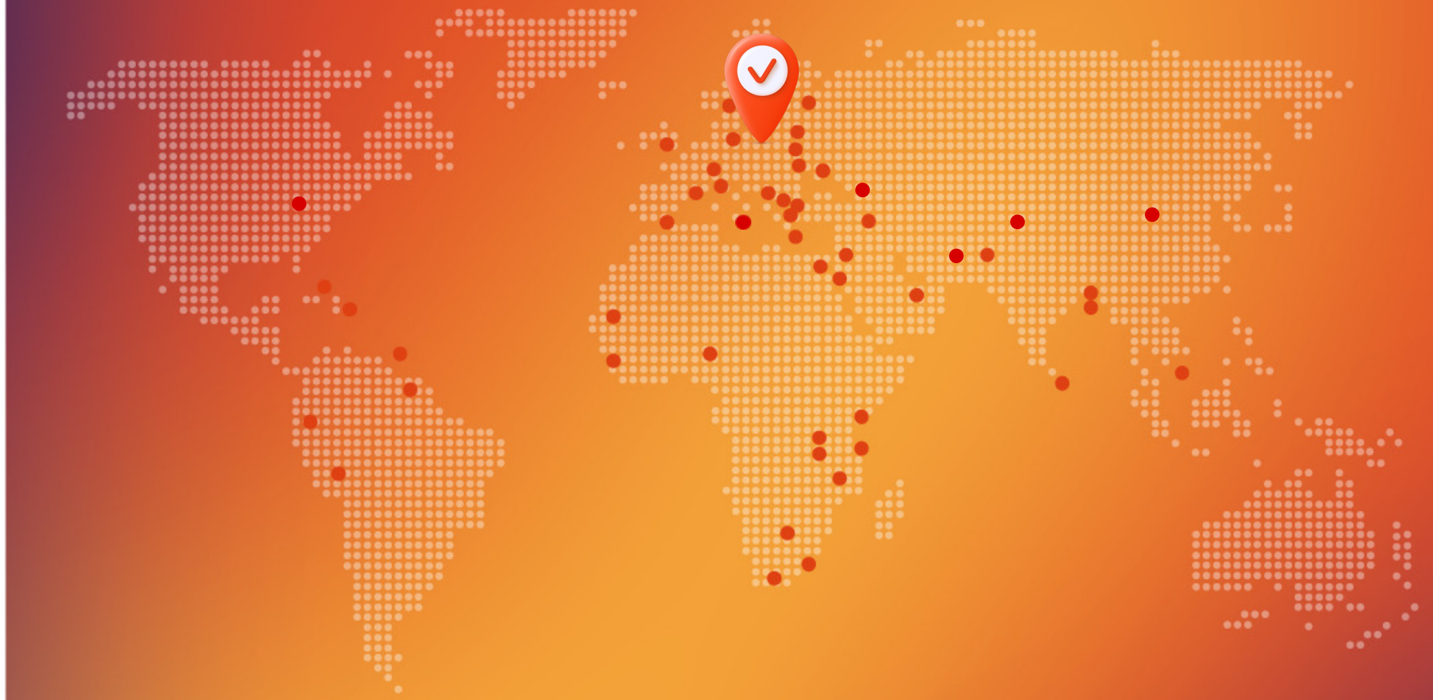
Cybersecurity operations build-out, incident detection and handling, establishment and support of Computer Security Incident Response Teams (CSIRTs) and Security Operation Centres (SOCs), and cyber capacity enhancement for organisations, sectors, and nations.

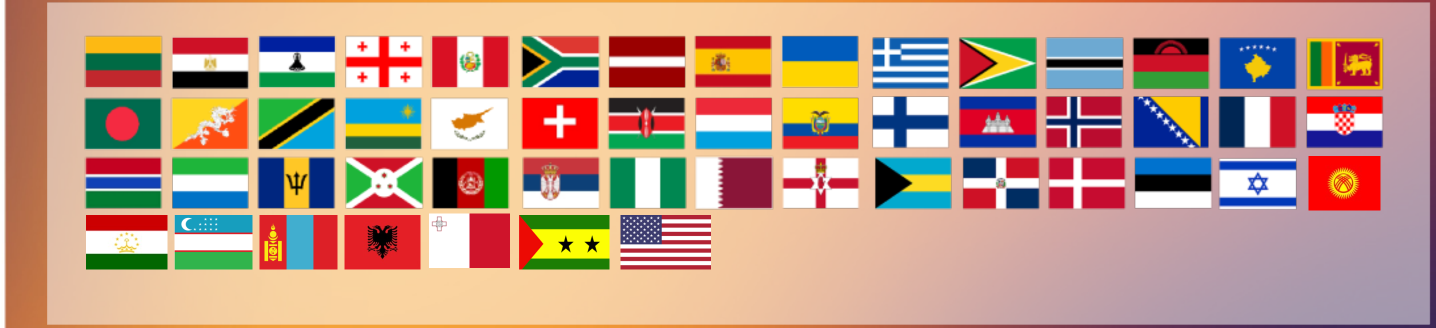
CUSTOMERS

Governments, public, and private sector organisations.

We are based in
Lithuania

Project geography





CSIRT/SOC establishment and modernisation projects

National level

Malta: The National CSIRT modernisation (*on-going*)

The Bahamas: The National CIRT establishment (*on-going*)

Malawi: The National CERT establishment

Barbados: The National CSIRT modernisation

Kenya: The National CSIRT modernisation

Afghanistan: Assessment of current maturity of AF-CERT and the design of way forward

Cyprus: National CSIRT establishment

Bhutan: National CIRT development

Bangladesh: BGD e-Gov CIRT establishment

Sectorial level

Kosovo: E-CERT Sectorial CSIRT for energy sector

Egypt: EG-FinCIRT Sectorial CSIRT at Central Bank of Egypt

Nigeria: Cybersecurity Fusion Centre Capacity Building for the Central Bank of Nigeria

Uganda: Design for the sectorial C-SOC under the Uganda Bankers' Association

Organisational level

Peru: Secure soft SOC maturity assessment

South Africa: Growing cybersecurity maturity for the UCT

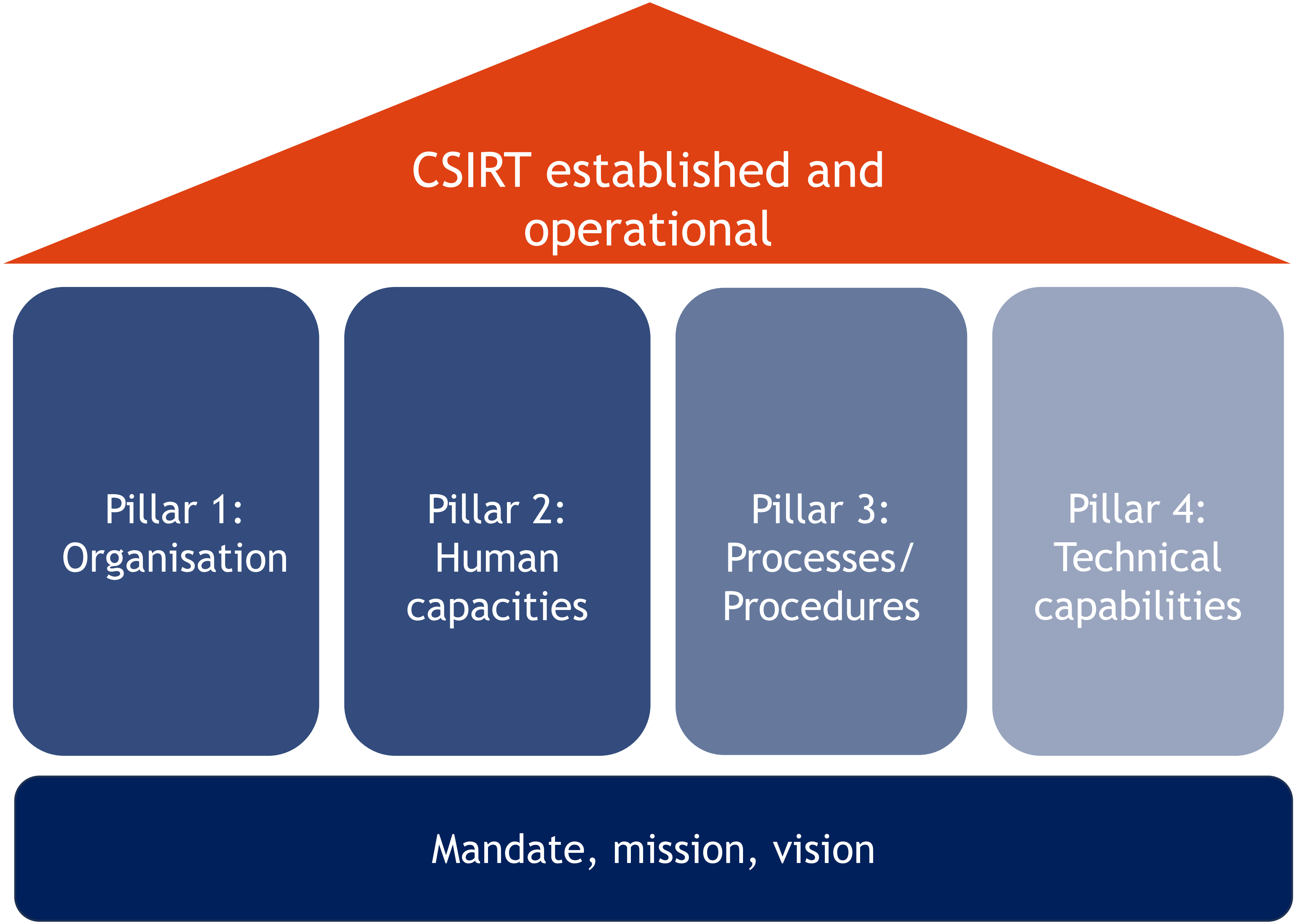
Training courses under ITU Academy

CSIRT/SOC establishment and modernisation

Incident response practice

> 100 attendees, 30 nationalities

Key pillars



CSIRT established and operational

Pillar 1: Organisation

Pillar 2: Human capacities

Pillar 3: Processes/ Procedures

Pillar 4: Technical capabilities

Mandate, mission, vision

Pillar 1: Organisation

Clear authority, legally defined powers

Established governance structure:

- ✓ Hosting organization
- ✓ Reporting structure

Sustainable funding model

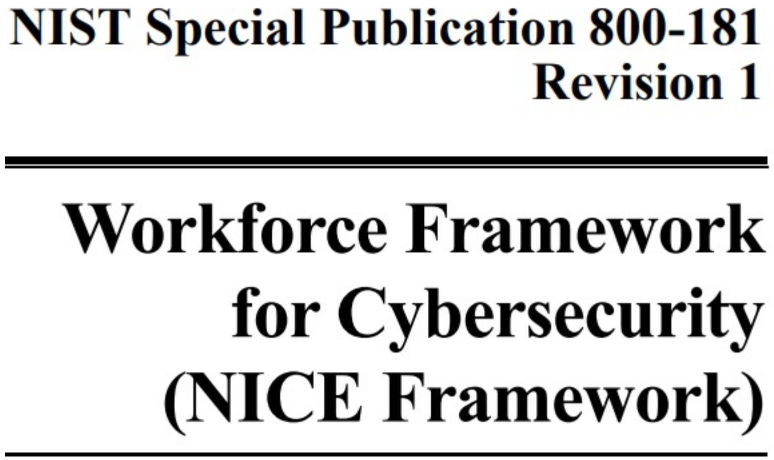
Pillar 2: Human capacities

Hiring skilled and competent staff

Staff training plan:

- ✓ Hosting organization
- ✓ Reporting structure

Staff retention plan

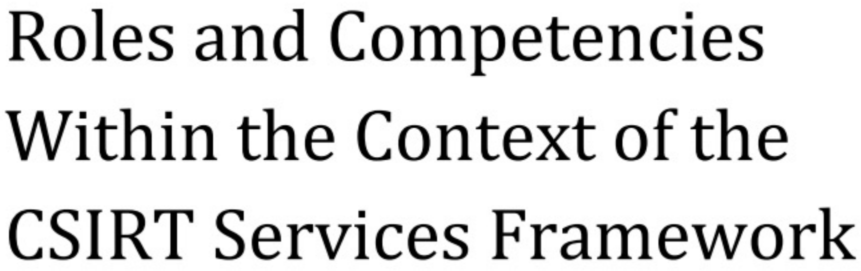


NIST Special Publication 800-181
Revision 1

Workforce Framework
for Cybersecurity
(NICE Framework)

FIRST™ Forum of Incident Response and Security Teams

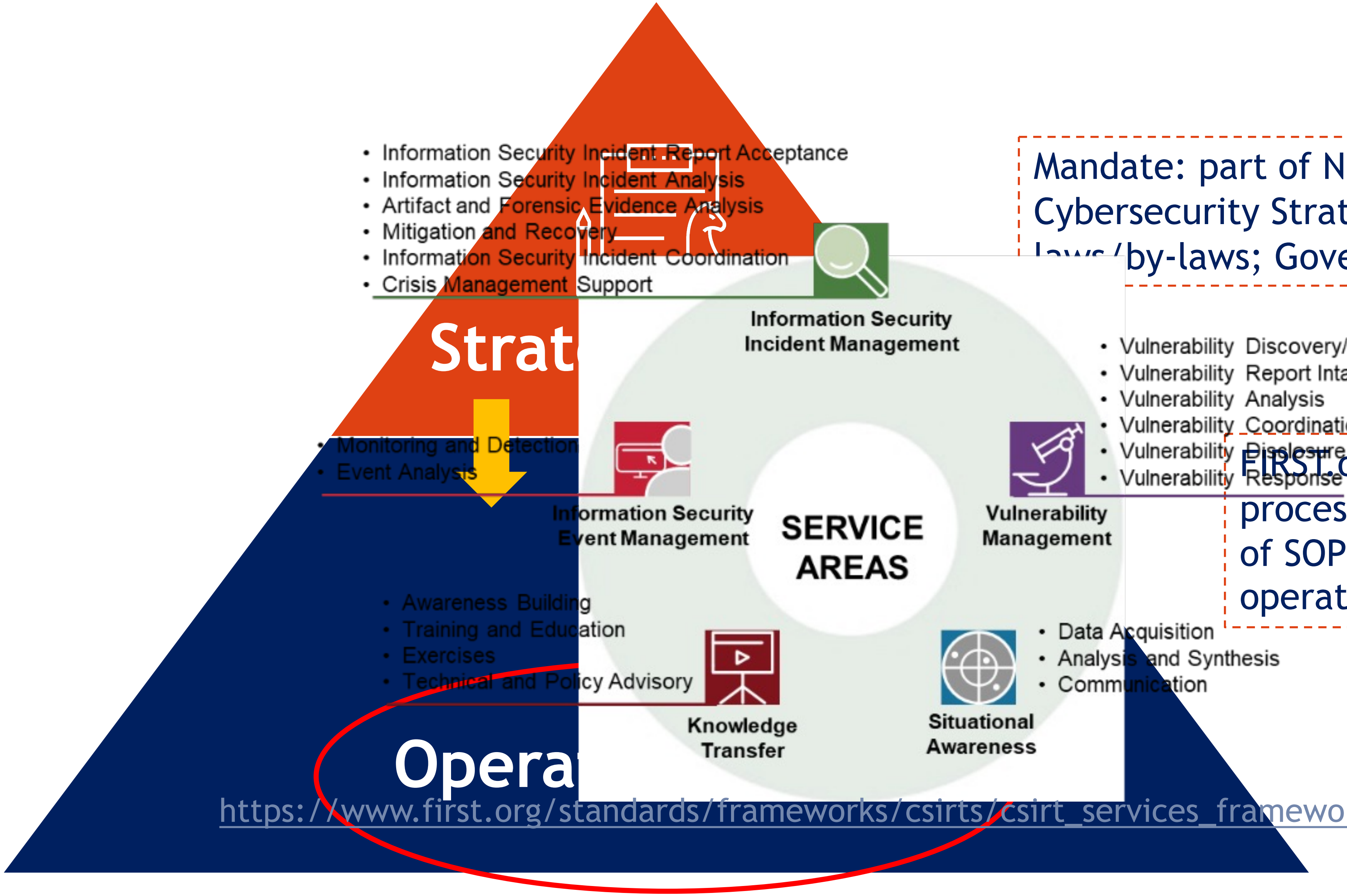
Improving Security Together



Roles and Competencies
Within the Context of the
CSIRT Services Framework

Pillar 3: Processes and Procedures

Operational level: CSIRT Services



- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- Information Security Incident Coordination
- Crisis Management Support

- Monitoring and Detection
- Event Analysis

- Vulnerability Discovery/Research
- Vulnerability Report Intake
- Vulnerability Analysis
- Vulnerability Coordination
- Vulnerability Disclosure
- Vulnerability Response

- Awareness Building
- Training and Education
- Exercises
- Technical and Policy Advisory

- Data Acquisition
- Analysis and Synthesis
- Communication

Mandate: part of National Cybersecurity Strategy; laws/by-laws; Government order

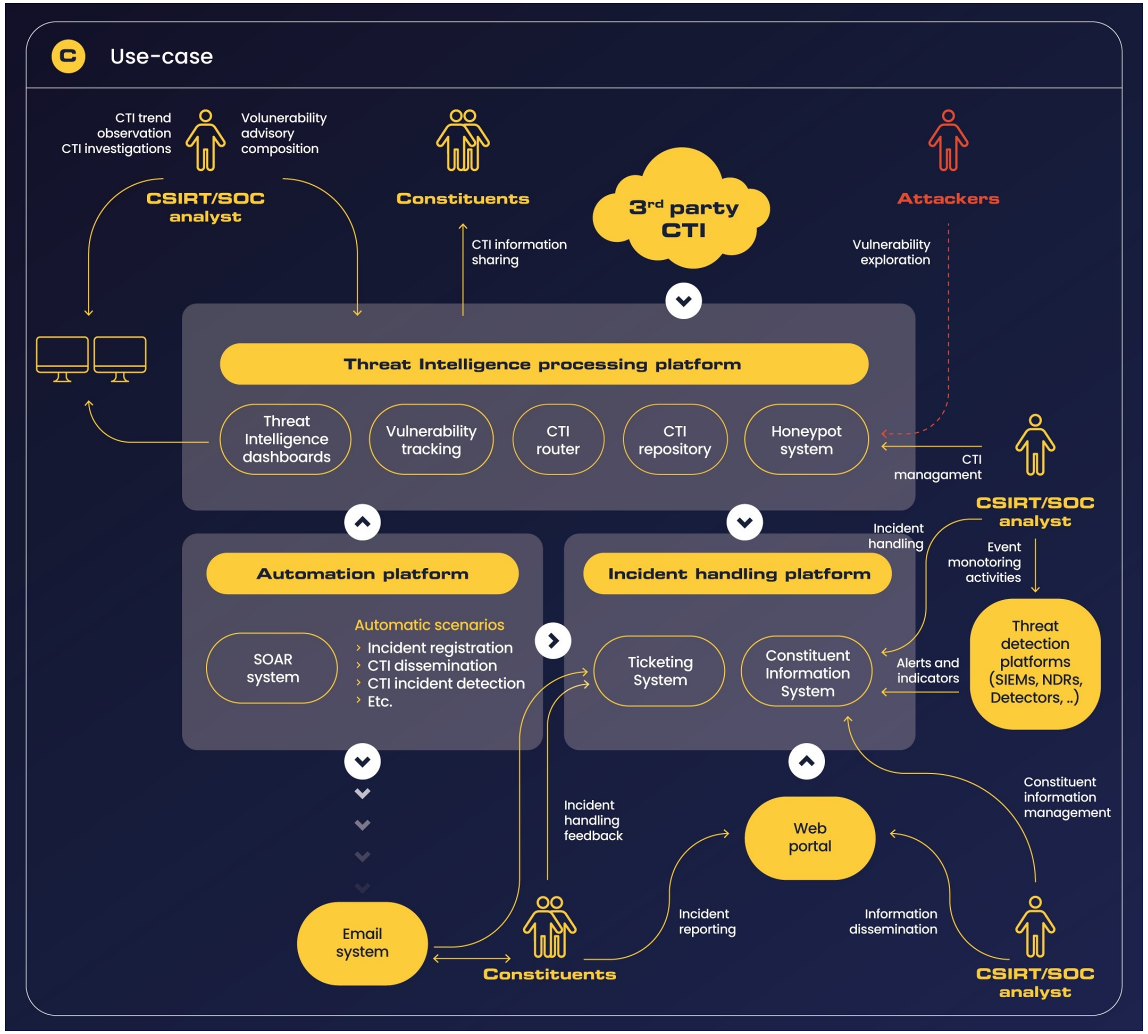
FIRST.org Service Model services, processes and procedures: part of SOPs, internal policies, operational workflows

https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Pillar 4: Technical capabilities

Automation in CSIRTs:

- Security monitoring workflows Incident management workflows
- Vulnerability management workflows
- Threat intelligence workflows
- Digital forensics and artifact analysis workflows – Awareness, training and risk analysis workflows - Infrastructure management workflows


Use-case
CTI trend observation
CTI investigations
Voluneraility advisory composition
CSIRT/SOC analyst
Constituents
CTI information sharing
3rd party CTI
Attackers
Vulnerability exploration
Threat Intelligence processing platform
Threat Intelligence dashboards
Vulnerability tracking
CTI router
CTI repository
Honeypot system
CTI managament
CSIRT/SOC analyst
Incident handling
Event monotoring activities
Automation platform
Incident handling platform
Automatic scenarios
Incident registration
CTI dissemination
CTI incident detection
Etc.
SOAR system
Ticketing System
Constituent Information System
Alerts and indicators
Threat detection platforms (SIEMs, NDRs, Detectors, ..)
Constituent information management
Incident handling feedback
Web portal
Incident reporting
Information dissemination
Email system
Constituents
CSIRT/SOC analyst